California Public Employees’ Retirement System

PERS-HRD-88 (Rev. 1/06)

Please refer to JOB #6977/JH on the application

POSITION DUTY STATEMENT

Title of Position
SAS User Access Analyst, User Access Team

Division and/or Subdivision
Information Technology Services Branch/Security Administration Services

Location of Headquarters
400 Q Street, Sacramento, CA 95814

INSTRUCTIONS: The Executive Officer is required by Government Code Section 18805 to report (or to record) “... material changes in the duties of any position in his jurisdiction.” The Position Duty Statement is used for this purpose. Enter identifying information and effective date at the right. Enter brief description of each of the important duties and responsibilities of the position below. Group related duties in numbered paragraphs and indicate the proportion of work time occupied. Prepare copies for employee assigned to the position and his/her supervisor.

Class Title of Position
Associate Information Systems Analyst (Specialist)

Position Number
275-815-1470-733(4003)

Effective Date
7/1/2010

Percent of Time Required	Effective on the date indicated, the employee assigned to the position identified above performs the following duties and responsibilities:
	As a user access analyst for the User Access Team (UAT), under the general supervision of the Senior Information Systems Analyst (Supervisor), within the Security Administration Services (SAS) unit of the Information Technology Services Branch (ITSB), the Associate Information Systems Analyst (AISA) (Specialist) performs a variety of functions related to user access security administration. This includes the analysis, development, implementation, and ongoing maintenance of user access processes in support of CalPERS business needs, information security policies, as well as, State/Federal legal mandates. Duties will include the following:
45%	Provide technical security administration and user access activities for ITSB’s information systems. This includes, but is not limited, to the following: • Scheduling work assignments to ensure adequate coverage and customer service is provided. • Add, modify, and delete users’ access permissions on all systems for which the UAT is responsible. • Work with users to define/maintain access groups that are appropriate for users’ job functions. • Process Exit Clearances: Collect security equipment from users; prepare/issue revocation notices to appropriate security administrators; revoke access on systems UAT is responsible for. • Provide technical troubleshooting and support for systems security problems. • Perform periodic reviews of user accounts on all CalPERS information systems to ensure removal of inactive accounts and verification of users' access authorization.
35%	Develop and implement user access monitoring processes and procedures for ITSB information systems and perform ongoing daily review of reports and logs to identify, analyze, and escalate security violations, intrusion attempts, and other security issues. Review existing processes and procedures and identify alternatives which will provide more effective and efficient monitoring.
10%	Plan and implement the transition of security administration for new systems and applications.
5%	Work with team lead to develop UAT workload measurements and workload monitoring processes. Report workload metrics to management on a regular basis.
5%	Maintain and enhance information security knowledge through formal/informal training, participation in security-related organizations, reading, and research.